世界知的所有権機関
国際事務局

**PCT**

特許協力条約に基づいて公開された国際出願

| | | | |
|---|---|---|---|
| (51) 国際特許分類7<br>**H04L 9/30, 9/08, G09C 1/00** | **A1** | (11) 国際公開番号 | **WO00/45548** |
| | | (43) 国際公開日 | 2000年8月3日(03.08.00) |

(21) 国際出願番号 PCT/JP00/00475

(22) 国際出願日 2000年1月28日(28.01.00)

(30) 優先権データ

| | | |
|---|---|---|
| 特願平11/21254 | 1999年1月29日(29.01.99) | JP |
| 特願平11/239177 | 1999年8月26日(26.08.99) | JP |


(71) 出願人（米国を除くすべての指定国について）
株式会社 日立製作所(HITACHI, LTD.)[JP/JP]
〒101-8010 東京都千代田区神田駿河台四丁目6番地
Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
西岡玄次(NISHIOKA, Mototsugu)[JP/JP]
〒215-0013 神奈川県川崎市麻生区王禅寺1099番地
株式会社 日立製作所 システム開発研究所内 Kanagawa, (JP)
(74) 代理人
弁理士 作田康夫(SAKUTA, Yasuo)
〒100-8220 東京都千代田区丸の内一丁目5番1号
株式会社 日立製作所内 Tokyo, (JP)

(81) 指定国 AU, CN, JP, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

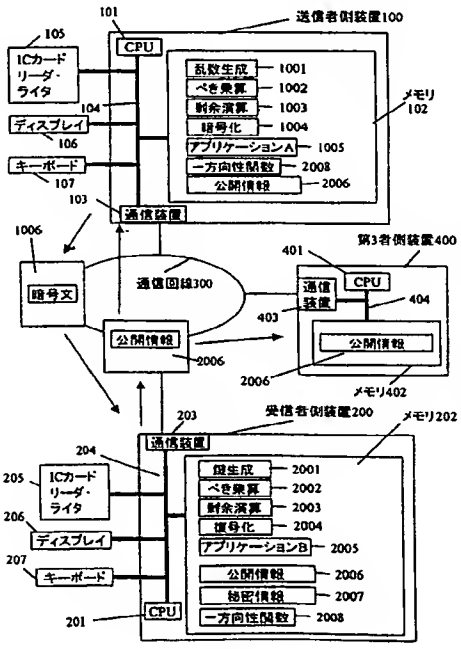
添付公開書類
国際調査報告書

(54)Title: **PUBLIC KEY CRYPTOGRAPH AND KEY SHARING METIIOD**

(54)発明の名称 公開鍵暗号及び鍵共有方法

**(57) Abstract**

A cryptograph communication method using public key cryptograph in which a sender creates a cryptogram by using a public key of the receiver by means of a sender device (100) and transmits it to the receiver device (200) through a communication line (300), and the receiver decrypts the cryptogram by using a secret key, wherein a procedure for encryption and decryption is so established to providc the features of security both the Rabin cryptograph which is one-way against chosen-plaintext attacks on the condition of difficulty of the problem of fractionization into prime factors and the ElGamal cryptograph which is strongly secret against chosen plaintext attacks on the condition of difficulty of the problem of Diffie-Hellman determination. Further while keeping secret the true plaintext space, the size of the plaintext space is reduced in order to use the space for key delivery of common key cryptogram. Thus a public key encrypting method and a key sharing method using the same are provided in which it is possible to prove the security on thc condition of the problem more difficult than conventional, and high efficiency processing in the calculation for encryption/decryption is possible.




105...IC CARD READER/WRITER
106...DISPLAY
107...KEYBOARD
100...SENDER DEVICE
1001...RANDOM NUMBER GENERATION
1002...EXPONENTIATION
1003...REMAINDER CALCULATION
1004...ENCRYPTION
1005...APPLICATION A
2008...ONE-WAY FUNCTION
2006...PUBLIC INFORMATION
102...MEMORY
103...COMMUNICATION DEVICE
1006...CRYPTOGRAM
2006...PUBLIC INFORMATION
300...COMMUNICATION LINE
400...THIRD-PARTY DEVICE
403...COMMUNICATION DEVICE
2006...PUBLIC INFORMATION
402...MEMORY
205...IC CARD READER/WRITER
206...DISPLAY
207...KEYBOARD
203...COMMUNICATION DEVICE
200...RECEIVER DEVICE
202...MEMORY
2001...KEY GENERATION
2002...EXPONENTIATION
2003...REMAINDER CALCULATION
2004...DECRYPTION
2005...APPLICATION B
2006...PUBLIC INFORMATION
2007...SECRET INFORMATION
2008...ONE-WAY FUNCTION

(57)要約

送信者は受信者の公開鍵を用いて送信者側装置100内で暗号文を作成し，通信回線300を介して受信者側装置200に送信し，受信者は秘密鍵を用いて暗号文の復号化を行う公開鍵暗号による暗号通信方法であって，素因数分解問題の困難性を前提に選択平文攻撃に対して一方向であるRabin暗号と，Diffie-Hellman決定問題の困難性を前提に選択平文攻撃に対して強秘匿であるElGamal暗号の双方の安全性の特徴を併せ持つように，暗号化および復号化のための手順を構築する。さらに，共通鍵暗号の鍵配送に使用する目的の下で，真の平文空間を秘密にしながら，平文空間の大きさを小さくする。これにより、従来方式に対して，より困難な問題を前提に安全性の証明が可能であり，かつ，暗復号化のための計算において効率性の高い処理ができる公開鍵暗号方法とそれを用いた鍵共有方法を提供する。

# 明 細 書

## 公開鍵暗号及び鍵共有方法

### 背景技術

本発明は，公開鍵暗号を用いた暗号通信方法および鍵共有方法に関する。

現在まで，様々な公開鍵暗号方式が提案されている。なかでも，

・文献1「R.L.Rivest, A.Shamir, L.Adleman:A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1978.」に掲載されている方法が最も有名であり，最も実用化されている公開鍵暗号である。

その他には，

・文献2「V.S.Miller:Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS218, Springer-Verlag, pp.417-426 (1985)」，

・文献3「N.Koblitz: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987)」等に記載の楕円曲線を用いた方法が効率的な公開鍵暗号として知られている。

安全性について証明可能な方法として，まず，選択平文攻撃を対象としたものは，

・文献4「M.O.Rabin: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」に記載されている暗号方法，

・文献5「T.ElGamal:A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp.469-472(1985)」に記載されている暗号方法,

・文献6「S.Goldwasser and S.Micali: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984) 」に記載されている暗号方法,

・文献7「M.Blum and S.Goldwasser: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS196, Springer-Verlag, pp.289-299 (1985)」に記載されている暗号方法,

・文献8「S.Goldwasser and M.Bellare: Lecture Notes on Cryptography, http:/www-cse.ucsd.edu/users/ mihir/ (1997)」に記載されている暗号方法,

・文献9「T.Okamoto and S.Uchiyama.A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS1403, Springer Verlag, pp.308-318 (1998)」に記載されている暗号方法, などが知られている。

また, 選択暗号文攻撃に対して安全性証明可能な方法としては,

・文献10「D.Dolve, C.Dwork and M.Naor.:Non-malleable cryptography, In 23rd Annual ACM Symposium on Theory of Computing, pp.542-552 (1991)」に記載されている暗号方法,

・文献11「M.Naor and M.Yung.:Public-key cryptosystems provably secure against chosen ciphertext attacks, Proc. of STOC, ACM Press, pp.427-437 (1990)」に記載されている暗号方法,

・文献12「M.Bellare and P.Rogaway,.Optimal Asymmetric En-

cryption – How to Encrypt with RSA, Proc. of Eurocrypt'94, LNCS950, Springer Verlag, pp.92-111 (1994)」に記載されている暗号方法,

・文献13「R.Cramer and V.Shoup: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS1462, Springer-Verlag, pp.13-25 (1998)」に記載されている暗号方法, などが知られている。

また,

・文献14「M.Bellare, A.Desai, D.Pointcheval and P.Rogaway. : Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNCS1462, Springer Verlag, pp.26-45 (1998)」では, IND-CCA2 (適応的選択暗号文攻撃に対して強秘匿であること) とNM-CCA2 (適応的選択暗号文攻撃に対して頑強であること) の等価性が示され, 現在, この条件を満たす公開鍵暗号が最も安全であると考えられている。

文献1に開示されている暗号方法の安全性は, 素因数分解問題の困難性を仮定しているが, 等価性は示されていない。すなわち, 素因数分解問題を解ければ文献1の暗号方法を破ることできるが, 逆は証明されていない。素因数分解問題よりも簡単な問題を解くことで文献1の暗号方法を破ることが出来る可能性は残されている。

さらに文献1の暗号方法は, 確定的な暗号であるため、鍵が同一である場合, 同一の平文に対する暗号文は常に同一になる。そのままで使用すると, 複数の暗号文から平文の同一性を判断することが可能になるので、これを防ぐためには運用時は乱数情報を付加するという別処理が必要になり、効率が悪い。

これに対して，文献９に開示されている暗号方法では，受動的攻撃に対して暗号文から平文を求めること（完全解読）は素因数分解問題の困難性と等価であることが証明されており，これにより安全性を保証している。さらに，同一の平文であっても暗号文が変化する確率暗号であるため，文献1の暗号方法のような問題や、別処理の必要性はない。

また、文献９の暗号方法における部分解読に対する安全性(semantic security)は，文献９中にて定義されているp-部分群問題の困難性と等価であるとして、その安全性が主張されている。しかしながら、この問題は未だ十分な議論がなされておらず，その困難性については知られていない。つまり，p-部分群問題を解く効率的なアルゴリズムが見つかれば，文献９の暗号方法の部分解読を効率的に行うことが出来てしまい、その安全性は保証できなくなる。

一般に，暗号の安全性を保証するためには，素因数分解問題や離散対数問題など計算量的困難性について十分議論されている問題との等価性を示すことが望ましい。

また、文献13に記載の暗号方法は、文献５に記載の暗号方法を用いて作成した暗号文に、暗号前のメッセージを知らないと作成できない「メッセージ情報」を付与するものである。このメッセージ情報が暗号文に対応する場合だけ正当な暗号文として対処し，そうでない場合は拒否するという仕組みであり、このメッセージ情報処理の処理量が多い。

一方、携帯型情報処理機器の普及やネットワーク環境の発展などにより、これら携帯型情報処理機器を用いて電子商取引を行うことが増えてくると予想されている。これら情報機器においては、計算能力が限られている反面、電子商取引では、複雑なプロトコルのために、元々データ量が多い。したがって、暗号化に伴うデータ量を減らすよりは、計算負荷を減らす方が望まれる場合がある。

発明の開示

本発明の目的は，安全性の証明が可能であり，かつ，暗復号化処理の効率性に優れる公開鍵暗号方法を提供することにある。

本発明では，従来から知られている暗号方法に比べて，より困難な問題の計算量的複雑さを前提としてOW-CPA（選択平文攻撃に対して一方向）かつIND-CPA（選択平文攻撃に対して強秘匿）であることが証明可能な公開鍵暗号方法を提供する。さらに，この方法をベースに，IND-CCA2またはNM-CCA2であることが証明可能な公開鍵暗号方法を提供する。

本発明による暗号方法は，従来技術に比べて，暗復号化処理の際に計算量が多くなるモジュラー積の個数が少なく，高速な処理が可能となる。

また，本発明の他の目的は，送信データを暗号化する際の計算および暗号化データを復号化する際の計算の負荷が小さく，携帯型情報処理機器など計算能力が限られた装置であっても高速処理が可能な，公開鍵を用いた暗号化方法と復号化方法と，それを用いた鍵配送方法や鍵共有方法，さらには，これらの方法を実行するプログラム，装置またはシステムを提供することである。

上記目的を達成するため，本発明は以下の手段を備える。

（１）文献４に記載の暗号方法（Rabin暗号）が持つ、選択平文攻撃に対して一方向性（OW-CPA）が証明可能な特徴と，文献５に記載の方法（ElGamal暗号）が持つ選択平文攻撃に対して強秘匿性（IND-CPA）が証明可能な特徴、とを持つように暗号化および復号化のための手順を構築し，さらに秘密情報を知られることなく平文空間を小さく選ぶ。

具体的には、暗号系が定義される有限群 $G=(Z/n)^*$ （$n=p^dq$）に対して，平文空間を$(0, 2^{k-2})$とする（但し，$k=|pq|$）。

（２）上記（１）で述べた公開鍵暗号方法に対して，（理想的）ランダ

ム関数が公開されていることを前提に，平文および乱数情報に対して，排他的論理和およびデータの連接による演算を行い，それらをランダム関数Hに入力した値を計算し，さらに，平文および乱数情報とランダム関数への入力値に対して排他的論理和およびデータの連接による演算を行う。

具体的な方法の1つとしては，

[鍵生成]

- $p$, $q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成し，さらに，

- $\alpha, g, h, k, l \in \mathbb{Z}$ $(0 < g, h < n)$
- $n = p^d q$ ($d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）を作成し（但し，kはpqのビット長）。

[暗号化]

送信者は，平文m（$m \in \{0,1\}^{\delta}$）に対して，

$$m_1 = (m0^{k_1} \oplus G(r)) \,||\, (r \oplus H(m0^{k_1} \oplus G(r))) \qquad (0 < m_1 < 2^{k-2})$$

を計算し（但し，$0<r<2^{k0}$，$G:\{0,1\}^{k0} \rightarrow \{0,1\}^{\delta+k1}$，$H:\{0,1\}^{\delta+k1} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$0<m_1<2^{k-2}$とする。），さらにJacobi記号$a=(m_1/n)$，および，

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n$$

を計算し，(C, D, a)を暗号文として受信者に送信する。

[復号化]

受信者は，自身の秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxを$m'_1$として計算する。但し，$\phi$は中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。

さらに，$m'_1=s'||t'$（s'は$m'_1$の上位nビット，t'は下位$k_0$ビット）に対して，

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする。（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。）

また，復号結果が * であるとは，正しい復号ができなかったことを意味する。ある暗号文に対して，正しい復号ができなかった場合、その暗号文が攻撃のためのものである可能性がある。したがって、復号結果である平文メッセージを出力しない構成にすれば、選択暗号文攻撃を退けることができる。

なお、実際には、理想的ランダム関数の仮定は非現実的であるため、実用的な一方向性関数を用いて、実用性と安全性とを確保した暗号を構成している。実用的な一方向性関数を用いた暗号と、理想的ランダム関数を仮定した暗号との安全性の差を明らかにすることは今後の課題とされている。しかしながら、実用的な一方向性関数を用いた暗号も、安全

性が証明された暗号方式の近似版であるため、ある種の安全性の保証があると予想されている。「岡本、藤崎、内山：安全性が証明された新しい公開鍵暗号、情報処理４０巻２号、pp170,173、(1999.2)」

図面の簡単な説明

第１図は、本発明の各実施例のシステム構成を示す図である。

第２図は、本発明の実施例における計算機能付き記憶媒体の内部構成を示す図である。

第３図は、本発明と代表的な実用的公開鍵暗号との効率性（モジュラー積の個数）および安全性の比較を示す図である。

発明を実施するための最良の形態

以下の実施例では、上記暗号化者を送信者、復号化者を受信者、暗号化の対象となる平文データを送信データともいい、メッセージの送信者Ａと受信者Ｂとが、それぞれ、送信者側装置、受信者側装置を用いて、送信データを暗号通信する場合について説明する。

第１図は，本発明の各実施例を実現するシステム構成を示す図であって、ネットワーク(通信回線ともいう)300に暗号化者が使用するコンピュータ（暗号化者側装置、または送信者側装置ともいう）100、および、復号化者が使用するコンピュータ（復号化者側装置、または受信者側装置ともいう）200、および、第３者が使用するコンピュータ（第３者側装置ともいう）400が接続されている。

暗号化者側装置100、復号化者側装置200は、それぞれCPU(101、201)、半導体記憶装置やハードディスクなどの二次記憶装置で構成されるメモリ(102、202)、通信装置(103、203)、バス(104、204)によって構成され、さらにディスプレイ(106、206)、および、キーボード(107、

207)がバス(104、204)に接続されている。また、暗号化者、復号化者が所有するICカードと通信をすることができるICカードリーダ・ライタ105,205がバス104,204に接続されている。

暗号化者側装置100のメモリ102には、以下の各実施例に示す各種情報と、CPU101が実行するプログラム（手段という）と、キーボード107や可搬型記憶媒体または通信回線300を介して入力されて暗号化の対象となる平文データ（送信データ）と、送信される暗号文とが保存される。

復号化者側装置200のメモリ202には、以下の各実施例に示す各種情報と、CPU201が実行するプログラム（手段という）と、復号化の対象となる暗号文と、復号化されてディスプレイ206や通信回線300に出力される平文データ（送信データ）とが保存される。

本発明の各実施例において、受信者は，受信者側装置200内の鍵生成手段2001を用いて、秘密情報と公開情報を作成する。公開情報は、通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者側装置400を有する公開情報管理機関への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ202に格納する。

送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いた乱数生成や、第３者装置400あるいは受信者側装置200から得られる公開情報2006を基にした計算を，べき乗算手段1002，剰余演算手段1003を用いて行う。さらに，暗号文は、通信装置103を用いて通信回線300を介して受信者側装置200に送信することができる。

受信者側装置200内の復号化手段2004は、受信した暗号文の復号化を、保持されている上記秘密情報2007を基に、べき乗算手段2002，剰余演算手段2003を用いて行う。

以下の実施例で述べる各手段が行なう処理は、直接又は間接的に、各

装置の操作者(送信者、受信者)の指示により、行なわれるものである。

(実施例 1)

本実施例は，メッセージの送信者であるAが受信者であるBに対して，送信データmを暗号通信によって送信する場合について説明する。

1．鍵生成処理

受信者Bは，予め，

- $H$：$G$ の部分群
- $s \in \mathbb{Z}$，$gh^s = 1$ $(\in G)$
- $\alpha^{-1} \in \mathbb{Z}$

なる秘密情報（H, s, $\alpha^{-1}$）を作成し（但し，$\alpha^{-1}$は有限群Hの位数を法とする環における$\alpha$の逆元），

- $G$：有限アーベル群
- $H'$：$H$ の部分集合
- $g, h \in G$
- $\alpha \in \mathbb{Z}$

なる公開情報（G, H', g, h, $\alpha$）を作成する。

2．暗復号化処理

（1）送信者Aは，平文m($\in$H')に対して，乱数rを生成し，さらに

$$C = m^{\alpha} g^{r}, \quad D = h^{r} \quad (\in G)$$

を計算する。

さらに，第3者あるいは受信者Bから上記公開情報を得て，暗号文から平文が一意的に復号化されるための付加情報aを計算する。

さらに，暗号文(C, D, a)を受信者側装置200に送信する。

（2）受信者Bは，保持している上記秘密情報（s, $\alpha^{-1}$）を用いて暗号文(C, D, a)から，

$$\tilde{m} = (CD^s)^{\alpha^{-1}} \quad (\in H)$$

を計算し，さらに付加情報aから元の平文mを計算する。

（実施例 2）

本実施例は，実施例1において，有限アーベル群G，Hの与え方，および，付加情報aの作成方法を具体的に示すものである。

1．鍵生成処理

受信者Bは，予め，

- $p, q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密情報（p, q, s, $\beta$）を作成し，

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$
- $n = p^d q \qquad (d$ は奇数$)$

なる公開情報（n, g, h, k, l, $\alpha$）を作成する。（但し，kはpqのビット長）

2．暗復号化処理

（1）送信者Aは，平文m($0<m<2^{k-2}$)に対して，乱数r（$0 \leqq r \leqq 1$）を生成し，さらに，

$$C = m^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n$$

を計算する。

さらに，上記公開情報を得て，Jacobi記号a=(m/n)を計算する（Jacobi記号の定義および計算方法については，例えば文献「高木貞

治：初等整数論講義，岩波書店」に記載されている）。

さらに，暗号文(C, D, a)を受信者側装置200に送信する。

（２）受信者Ｂは，保持している上記秘密情報（p, q, s, $\beta$）を用いて暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p}, m_{1,q})$，$\phi(-m_{1,p}, m_{1,q})$，$\phi(m_{1,p}, -m_{1,q})$，$\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすものを平文mとする（但し，$\phi$は中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す。）。

本実施例による方法では、選択平文攻撃に対して，一方向であること，および，強秘匿であることが証明できる。

具体的には、nの素因数分解問題よりも困難な問題の困難性を前提として完全解読が不可能なことを示すことができる。すなわち，ある（nの素因数分解問題よりも困難な）問題を解くアルゴリズムが存在すれば，そのアルゴリズムを利用して本実施例の方法の完全解読を行うアルゴリズムを構成することができる。また，本実施例の方法の完全解読を行うアルゴリズムが存在すれば，そのアルゴリズムを利用して，ある（nの素因数分解問題よりも困難な）問題を解くアルゴリズムを構成することができる。

さらに，「条件付きのDiffie-Hellman決定問題」の困難性を前提として強秘匿であることを示すことができる。ここで，「条件付きのDiffie-Hellman決定問題」とは，確率分布

$$D_0 : (h, g, h^r, g^r), \quad 0 \le r \le l,$$
$$D_1 : (h, g, h^r, Xg^r), \quad X = (x/x')^{2\alpha} \bmod n,\ 0 < x, x' < 2^{k-2}$$

において，$D_0$または$D_1$からの任意のシーケンスに対して，いずれからのものであるかを言い当てる問題である。

本発明による方式において，暗号文（C, D, a）から平文 m を計算することは，素因数分解問題よりも困難であることが証明される。すなわち，本実施例において，暗号文（C, D, a）から平文 m を計算するアルゴリズムが存在すれば，このアルゴリズムを用いて素因数分解問題を解くアルゴリズムを構成できるということである。逆に，素因数分解問題を解くアルゴリズムが存在しても，これより本発明の暗号化方法において暗号文（C, D, a）から平文 m を計算するアルゴリズムは知られていない。この意味において，本発明の全文解読における安全性は素因数分解問題よりも困難である。

証明は，暗号文（C, D, a）から平文 m を計算するアルゴリズムに対して，適当な暗号文を入力し，その出力結果から無視できない確率で底となる合成数 n の素因数分解を行うという展開において，文献 4 に示される暗号方法における証明と類似している。以下に示す。

・暗号文（C, D, a）から平文 m を無視できない確率で計算することのできる確率的多項式時間アルゴリズム Adv が存在したとする。このとき，Adv をオラクルとして，n の素因数分解を無視できない確率で行う確率的多項式時間アルゴリズム A が構築できることを示す。

・A は提案方式における公開鍵（$\alpha$, n, g, h, l）に対して，$m' \in Z$ $(0<m'<2^{k-2})$，$r' \in Z$ $(0<r'<l)$ および $a' \in \{-1, 1\}$ を一様に選び，

$$C' = m' 2^{\alpha} g^{r'} \bmod n, \quad D' = h^{r'} \bmod n$$

を計算し，Adv に入力する。

・このとき，暗号文（C', D', a'）は正しい暗号文と同じ確率分布を持

つことから，Adv は無視できない確率で暗号文（C',D',a'）の平文を出力する。

・$m'^2 \bmod\{pq\}$ の平方根の４つ解を $m_1, m_2, m_3, m_4$ として，さらに $m_1+m_2\equiv 0 \bmod\{pq\}$ かつ $m_3+m_4\equiv 0 \bmod\{pq\}$ が成立すると仮定する。

・このとき，Adv における復号化において，暗号文（C',D',a'）の正しい平文の範囲が開区間（$0, 2^{k-2}$）であることから，候補は２つに絞られる。

・この残った２つの候補においては各々 Jacobi記号の値が異なることになる。よって，A が任意に選んだ a' に対して $(m'/n)\neq a'$ である場合，A はアルゴリズム Adv から未知の平文を得ることができる。

・よって，Adv の出力 m'' に対して，1/2 の確率で gcd(m'-m'',n) から n の素因数分解が得られる。

また，本発明による方式の部分解読に関する安全性は，制限付き Diffie-Hellman 決定問題の困難性と等価であり、その証明は、概ね，文献５に記載のElGamal暗号がDiffie-Hellman 決定問題の困難性を前提として強秘匿であることを証明する場合と同様である。

すなわち、「もし制限付きDiffie-Hellman 決定問題を解くアルゴリズムが存在すれば，無視できない確率でb∈{0,1}（encryption oracle が行ったコイントスの結果）を正しく推測するアルゴリズムを構成することができ，また，無視できない確率で b を正しく推測するアルゴリズムが存在すれば，それを用いて制限付きDiffie-Hellman 決定問題を解くことができる。」ことを示すことで証明する。

（実施例 3）

送信者が受信者に対し送信したいメッセージ文に対して，正しく復号されたかを確認するための検査情報を含むように平文mを作成すること

により、実施例１および実施例２の公開鍵暗号方法に、さらに、選択暗号文攻撃に対する対策を施すことができる。

具体的には、送信者が受信者に対し送信したいメッセージ文に対して，予め定められた冗長性を持たせた内容を平文mとし，実施例１（または実施例２）の方法により暗号化し，受信者は実施例１（または実施例２）の方法により平文m を復号化し，予め定められた冗長性を確認する（もし，予め定められた冗長性を持たない場合は，復号が正しく行われなかったものとみなす。）冗長性とは、例えば，送信したいメッセージを２回以上繰り返したものを平文とするなどの方法で、持たせることができる。

他の方法としては，送信者が受信者に対し送信したいメッセージ文に対して，予め定められた意味のあるメッセージを加えた内容を平文mとし，実施例１（または実施例２）の方法により暗号化し，受信者は実施例１（または実施例２）の方法により平文m を復号化し，予め定められた意味のあるメッセージの内容を確認する（もし，予め定められた意味のあるメッセージの内容が一致しない場合は，復号が正しく行われなかったものとみなす）。

なお、これらの処理手段は、暗号化手段1004、復号化手段2004に構成する。

このような方法により，実施例１および実施例２の公開鍵暗号方式は，選択暗号文攻撃に対しても，ある程度の安全性を確保することができる（選択暗号文攻撃に対して安全性が証明できる方法については，以下の実施例でも述べる）。

（実施例 4）

本実施例では，実施例１で述べた暗号通信方法を元に、さらに、実用的な一方向性関数を組み合わせるものである。これにより、送信者と受

信者の間で鍵共有を行うこと(すなわち、共通鍵暗号方法に用いる鍵を配送すること)を可能にする。また、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作り、能動的攻撃に対する安全性を確保する。

本実施例では、一方向性関数手段2008を新たに送信者側装置100内に設ける。また、配送された(または共有する)鍵を用いて、同時に、あるいは別途送受するデータを、おのおの暗号化、復号化する機能を有するアプリケーションAプログラム1005、アプリケーションBプログラム2005を、図1に示すように備えるものとする。

1．鍵生成処理

受信者Bは，実施例1と同様に、秘密情報（H, s, $\alpha^{-1}$）と公開情報（G, H', g, h, $\alpha$）を作成する。同時に公開情報として、一方向性関数fも定める。

2．鍵配送処理

送信者Aは，実施例1と同様に、暗号文(C, D, a)を計算し、受信者Bの受信者側装置200に送信する。また，一方向性関数手段2008を用いて、公開情報である一方向性関数fから，共有鍵K=f(m)を計算する。必要に応じて、アプリケーションAプログラム1005は、共通鍵Kを用いて暗号化計算を行う。

受信者Bは，実施例1と同様の手順にて、暗号文(C, D, a)から，元の平文mを計算し、さらに，一方向性関数手段2008を用いて、公開情報fから共有鍵KをK=f(m)により計算する。必要に応じて、アプリケーションBプログラム2005は、共通鍵Kを用いて復号化計算を行う。

上述の様に，本実施例では，一方向性関数を組み合わせて，使用することにより，送信データm自身は外部へ出力しない。したがって、送られてきた暗号文が攻撃のためのものであっても、選択暗号文攻撃を許さない，すなわち，能動的攻撃に対しても安全な環境を作ることができる。

また，メッセージそのものを本発明による公開鍵暗号方法を用いて送信する構成においては，本実施例のアプリケーションBプログラム2005が復号化したメッセージを所定のルールによって解釈し，意味のないメッセージが復号されたと判断した場合，そのメッセージを外部機器に出力することなく消去するなどして，能動的攻撃を許さない環境を作ることができる。

（実施例 5）

本実施例は，実施例４において述べた鍵共有方法について，実施例２で説明したような、有限アーベル群Ｇ，Ｈの与え方，および，付加情報ａの作成方法を具体的に示すものである。

１．鍵生成処理

受信者Ｂは，実施例２と同様に、秘密情報（p, q, s, $\beta$）と公開情報（n, g, h, k, l, $\alpha$）を作成（但し，kはpqのビット長）する。また、公開情報として、一方向性関数ｆも定める。

２．鍵配送処理

送信者Ａは，実施例２と同様の計算を行い、暗号文(C, D, a)を受信者側装置200に送信する。また，送信者は，実施例４と同様の計算を行い、一方向性関数ｆから，共有鍵K=f(m)を計算する。必要に応じて、アプリケーションAプログラム1005は、共通鍵Kを用いて暗号化計算を行う。

受信者Ｂは，実施例２と同様の計算を行い、平文mを求め、さらに、実施例４と同様の計算を行い、共有鍵K=f(m)を計算する。必要に応じて、アプリケーションBプログラム2005は、共通鍵Kを用いて復号化計算を行う

（実施例 6）

本実施例は，文献４に記載されている暗号方法をベースに，復号化処理を向上させることを目的として，$n=p^dq$（但し，ｄは３以上の奇数）

を法とする剰余環から決定される乗法群上で定義される方法に転換する。さらに，文献１２に記載の方法により，適応的選択暗号文攻撃に対して強秘匿であることが証明可能な公開鍵暗号方法へ転換する。

１．鍵生成処理

受信者Ｂは，予め、上記実施例と同様に、

- $p, q$：素数，　$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$，　$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密情報（p, q, $\beta$）を作成し，

- $\alpha, k \in \mathbb{Z}$
- $n = p^d q$　　($d$ は奇数)

なる公開情報（n, k, $\alpha$）（但し，ｋはｐｑのビット長を表す）を作成する。

２．暗復号化処理

（１）送信者Ａは，平文ｍ（$m \in \{0,1\}^{\delta}$）に対して，乱数ｒ（$0<r<2^{k0}$）を選び，さらに，

$$m_1 = (m0^{k_1} \oplus G(r)) \,||\, (r \oplus H(m0^{k_1} \oplus G(r))) \qquad (0 < m_1 < 2^{k-2})$$

を計算する。但し，$G:\{0,1\}^{k0} \rightarrow \{0,1\}^{\delta+k1}$，$H:\{0,1\}^{\delta+k1} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$0<m_1<2^{k-2}$とする。

さらに，上記公開情報を得て，Jacobi記号$a=(m_1/n)$，および，

$$C = m_1^{2\alpha} \bmod n,$$

を計算する。

さらに，暗号文（Ｃ，ａ）を受信者側装置200に送信する。

（２）受信者Ｂは，保持している上記秘密情報（p, q, $\beta$）を用いて暗号文(C, a)から，

$$m_{1,p} = C^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxを$m'_1$として計算する。但し，$\phi$は中国人の剰余定理による$Z/(p)\times Z/(q)$から$Z/(pq)$への環同型写像を表す。

さらに，演算手段204を用いて，$m'_1=s'||t'$（s'は$m'_1$の上位nビット，t'は下位$k_0$ビット）に対して，

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。また，復号結果が＊であるとは，正しい復号ができなかったことを意味する。）

ある暗号文に対して，正しい復号ができなかった場合、その暗号文が攻撃のためのものである可能性がある。したがって、受信者側装値200は、選択暗号文攻撃を不可能とするために、復号結果である平文メッセージは出力しない。このとき、受信者側装値200は、復号結果をなにも出力しない構成にしても良いし、または復号ができなかったという結果を通知する構成にしてもよい。

上記方法は、文献12において一般的な落し戸付き置換から構成される（決定性の）公開鍵暗号を対象に証明されているように、適応的選択暗号文攻撃に対して強秘匿であることがnの素因数分解問題の困難性との

等価性により証明することができる。

また，本実施例では，暗号化処理でのモジュラー積は３回（$\alpha = 3$の場合）であり，また，復号化処理においてはnよりも小さいpqを法とする剰余環から決定される乗法群の上で行うことにより，従来方法に比べて処理の高速性を実現している。

（実施例 7）

本実施例は，実施例２の方法を，文献１２に記載の方法により，適応的選択暗号文攻撃に対して強秘匿であることが証明可能な公開鍵暗号方法へ転換する。

１．鍵生成処理

実施例２と同様に行い、秘密情報（p, q, s, $\beta$）公開情報（n, g, h, k, l, $\alpha$）を作成する。

２．暗復号化処理

送信者Aは，実施例６と同様に、平文m（$0<m<2^{\delta}$）に対して，$m_1$を求める。さらに、実施例２における平文mに対する計算と同様にして、$m_1$についてC, Dを計算する。さらに，上記公開情報を得て，Jacobi記号$a=(m_1/n)$を計算し、暗号文（C, D, a）を受信者側装置200に送信する。

受信者Bは，上記秘密情報（p, q, s, $\beta$）を用いて暗号文(C, D, a)から，実施例２と同様の計算を行い、$m_{1,p}$, $m_{1,q}$を求め、

$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$

のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすものを$m'_1$とする。さらに，$m'_1=s'||t'$（s'は$m'_1$の上位nビット，t'は下位$k_0$ビット）に対して，

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする。

本実施例による方法では，nの素因数分解問題よりも困難な問題の困難性を前提として，IND-CCA2であることを示すことができる。

第１０図に，本発明の実施例８において$\alpha$=d=3とした場合と、代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）および安全性の比較を示す。また，本発明の方式における括弧の中の数字は前処理が可能である場合において前処理を行った結果である。なお，第１０図におけるデータの多くは，文献９から引用した。

（実施例 8）

本実施例は，実施例７の変形例である。

１．鍵生成処理

実施例７と同様に行い、秘密情報（p, q, s, $\beta$）公開情報（n, g, h, k, l, $\alpha$）を作成する。

２．暗復号化処理

送信者Ａは，平文m（$m \in \{0,1\}^{\delta}$）に対して，乱数r（$r \in \{0,1\}^{k0}$）を選び，さらに，

$$m_1 = (m \oplus G(r)) \,||\, (r \oplus H(m \oplus G(r))) \qquad (0 < m_1 < 2^{k-2})$$

を計算する。但し，$G:\{0,1\}^{k0} \rightarrow \{0,1\}^{\delta+k1}$，$H:\{0,1\}^{\delta+k1} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$0<m_1<2^{k-2}$とする。

さらに，上記公開情報を得て，Jacobi記号$a=(m_1/n)$，および，

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n$$

を計算する。但し，$F:\{0,1\}^{\delta+k0+k1} \rightarrow \{0,1\}^{l}$は適当なランダム関数である。

さらに，暗号文（C, D, a）を受信者側装置200に送信する。

受信者Ｂは，上記秘密情報（p, q, s, $\beta$）を用いて暗号文(C, D, a)から，

実施例７と同様の計算を行い、

$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすものを$m'_1$として求め、さらに，$m'_1=s'||t'$（$s'$は$m'_1$の上位nビット，$t'$は下位$k_0$ビット）に対して，

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする。但し，

$$C' = m_1'^{2\alpha} g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n$$

である。

本実施例による方法では，nの素因数分解問題よりも困難な問題の困難性を前提として，IND-CCA2であることを示すことができる。

また，本実施例の方法においては，実施例２の方法に比べて，平文を長くとることが可能である。

（実施例 9）

本実施例は，実施例７の変形例である。

１．鍵生成処理

実施例７と同様に行う。

２．暗復号化処理

送信者Ａは，平文m（$m \in \{0,1\}^{\delta}$）に対して，

乱数r（$r \in \{0,1\}^{k0}$）を選び，

$$m_1 = m \,||\, r$$

を計算する。但し，$F: \{0,1\}^{\delta+k0} \rightarrow \{0,1\}^{l}$は適当なランダム関数であり，$0<m_1<2^{k-2}$とする.

さらに，上記公開情報を得て， Jacobi記号a=($m_1$/n)，および，

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n$$

を計算する。

さらに，暗号文（C, D, a）を受信者側装置200に送信する。

受信者Bは，実施例8と同様に、上記秘密情報（p, q, s, $\beta$）を用いて暗号文(C, D, a)から，$m_{1,p}$, $m_{1,q}$を求め、

$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$

のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすものを$m'_1$とする。さらに，

$$m' = \begin{cases} [m'_1]^{k_0} & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする。但し，

$$C' = m_1'^{2\alpha} g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n$$

である。

本実施例による方法では，「条件付きDiffie-Hellman問題」の困難性を前提として，IND-CCA2であることを示すことができる。

また，本実施例の方法においては，実施例2の方法に比べて，平文を長くとることが可能である。

（実施例 10）

本実施例は，実施例8および実施例9において，受信者側の計算効率を高めるための復号化方法について述べる。

受信者は，

$$C'_p = m_1'^{2\alpha} g^{F(m_1')} \bmod p^d, \qquad C'_q = m_1'^{2\alpha} g^{F(m_1')} \bmod q$$
$$D'_p = h^{F(m_1')} \bmod p^d, \qquad D'_q = h^{F(m_1')} \bmod q$$

を計算し，さらに

$$C \equiv C'_p \pmod{p^d}, \qquad C \equiv C'_q \pmod{q},$$
$$D \equiv D'_p \pmod{p^d}, \qquad D \equiv D'_q \pmod{q}$$

により，(C, D)=(C', D')を検査する。

本実施例によれば、それぞれの計算において、剰余環から決定される乗法群を決定する底となる整数が小さくなるので、高速な処理が可能になる。

（実施例 11）

上記各実施例における暗号文の計算過程において、m'を、送信者が所持する計算機能付き記憶媒体500にて計算し、送信者側装置100に渡し、暗号文を計算することも可能である。

第２図は，計算機能付き記憶媒体500（例えばICカード、計算機カード）の内部構成を示す。計算機能付き記憶媒体500は， CPU501、半導体記憶装置などの記憶装置で構成されるメモリ502、I/O 503、バス504によって構成され、メモリ502には、各種情報と、CPU501が実行するプログラム（手段という）と、I/O 503を介して入力される、暗号化の対象となる平文データ（送信データ）が保存される。

以下の実施例においては、計算機能付き記憶媒体500内の暗号化手段5004が、メモリ502に保持されている上記公開情報2006と、べき乗算手段5002，剰余演算手段5003とを用いて，平文mから中間計算結果m'を計算し、送信者側装置100に渡す。

この方法によると、ICカード500の中で生成したメッセージmを，ICカード500を差し込む送信者側装置100にさえも知られることなく安全であり、かつ，送信者側装置100の高速な計算能力を利用して暗号文を作成することができるという特徴がある。

具体的には、実施例１および４においては、計算機能付き記憶媒体

500は，平文mから，

$$m' = m^{\alpha} \ (\in G)$$

を計算し，その結果m'を用いて送信者側装置100は，

$$C = m'g^{r}, \quad D = h^{r} \ (\in G)$$

により、暗号文を計算する。

実施例2および実施例5においては，計算機能付き記憶媒体500は，平文mから，

$$C = m'g^{r} \bmod n, \quad D = h^{r} \bmod n$$

を計算し，その結果m'を用いて送信者側装置100は，

$$C = m'g^{r} \bmod n, \quad D = h^{r} \bmod n$$

により、暗号文を計算する。

実施例7においては，計算機能付き記憶媒体500は，平文mから，

$$m_1' = m_1^{2\alpha} \bmod n$$

を計算し，その結果m'を用いて送信者側装置100は，

$$C = m_1'g^{r'} \bmod n, \quad D = h^{r'} \bmod n$$

により、暗号文を計算する。

実施例8および実施例9においては，計算機能付き記憶媒体500は，

平文mから，

$$m_1' = m_1^{2\alpha} \bmod n$$

を計算し，その結果m'を用いて送信者側装置100は，

$$C = m_1' g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n$$

により、暗号文を計算する。

上記各実施例において、d（d≧1）の値をnの素因数分解が困難である範囲において，大きく選ぶことで，nのビット数が一定の場合，pのビット数が小さくなるため，復号化処理を高速に行うことが出来る。dを、d>1なる奇数、とすれば、さらに効率を向上させることができる。

このdの値を、第3者側装置あるいは、受信者側装置にて管理すれば、計算機能力の発展、素因数分解に必要とされる計算時間と安全性との関係などによって、変えることが可能である。

上記各実施例に現れる，

$$g^r, h^r \quad (\in G)$$

または、

$$g^r \bmod n, \qquad h^r \bmod n$$

のように、暗号化対象である送信データm に関係しない計算は前処理が可能である。すなわち，これらの計算を前処理として行い，その結果を送信者側装置100の記憶手段（メモリ102など）に保存して，その値を読み出して用いることにより，暗号化時間を大幅に短縮する事ができる。

前処理を行うと，送信データm を用いた処理のモジュラー積の個数は1個となるため，暗号化時間を大幅に短縮することが可能となる。

また、上記各実施例における送信データm には、通常の秘密に送信したいメッセージのほか、共通鍵暗号方法に用いる共通鍵、メッセージ認証に用いるメッセージとメッセージ認証子を合わせたものが当てはまる。

また，本実施例では，送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが，具体的には様々なシステムに適用される。

以上の各実施例では，送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが，具体的には様々なシステムに適用される。

例えば，電子ショッピングシステムでは，送信者はユーザであり，送信者側装置はパソコンなどの計算機であり，受信者は小売店，受信者側装置はパソコンなどの計算機となる。このとき，ユーザの商品等の注文書は共通鍵暗号方法で暗号化されることが多く，その際は、暗号化鍵を本発明による鍵共有（鍵配送）方法により暗号化して小売店側装置に送信される。

また，電子メールシステムでは，各々の装置はパソコンなどの計算機であり，送信者のメッセージは共通鍵暗号方法で暗号化されることが多い。その際も、暗号化鍵は、本発明による鍵共有（鍵配送）方法を用いて暗号化して受信者の計算機に送信される。

その他にも，従来の公開鍵暗号が使われている様々なシステムに適用することが可能である。

なお、本実施例における各計算は、CPUがメモリ内の各プログラムを実行することにより行われるものとして説明したが、プログラムではなく、少なくとも一つが、ＬＳＩやハードウェア化された演算装置であっ

て、他の演算装置やCPUと、データのやりとりを行うものであってもよい。

産業上の利用可能性

本発明によれば，暗号攻撃に対して安全であり，また、高速処理が可能な，公開鍵暗号方法や，その様々な応用を提供することができる。

# 請 求 の 範 囲

1.

送信者は，公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

受信者は、受信者側装置を用いた鍵生成のステップとして，

- $H$ : $G$ の部分群
- $s \in \mathbf{Z}$, $gh^s = 1$ $(\in G)$
- $\alpha^{-1} \in \mathbf{Z}$

なる秘密鍵（H, s, $\alpha^{-1}$）を作成し（但し，$\alpha^{-1}$は有限群Hの位数を法とする環における$\alpha$の逆元），

- $G$ : 有限アーベル群
- $H'$ : $H$ の部分集合
- $g, h \in G$
- $\alpha \in \mathbf{Z}$

なる公開鍵（G, H', g, h, $\alpha$）を作成し，

送信者は，送信者側装置を用い、平文m($\in$H')および乱数rに対して，

$$C = m^{\alpha} g^{r}, \quad D = h^{r} \quad (\in G)$$

を計算し，暗号文から平文が一意的に復号化されるための付加情報aを計算し，(C, D, a)を暗号文として前記受信者に送信し，

前記受信者は，前記受信者側装置を用い、前記秘密鍵（s, $\alpha^{-1}$）を用いて，暗号文(C, D, a)から，

$$\bar{m} = (CD^{s})^{\alpha^{-1}} \quad (\in H)$$

を計算し，付加情報aから元の平文mを計算する
ことを特徴とする公開鍵暗号方法。

2．

送信者は，公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

受信者は、受信者側装置を用いた鍵生成のステップとして，

- $p, q$：素数，　$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，　$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，　$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成し，

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　($d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）を作成し（但し，kはpqのビット長），

送信者は，送信者側装置を用い、平文m（$0 < m < 2^{k-2}$）および乱数r（$0 \leqq r \leqq 1$）に対して，

$$C = m^{2\alpha} g^r \bmod n, \quad D = h^r \bmod n$$

を計算し，Jacobi記号a=(m/n)を計算し，(C, D, a)を暗号文として前記受信者に送信し，

前記受信者は，前記受信者側装置を用い、前記秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p}, m_{1,q})$，$\phi(-m_{1,p}, m_{1,q})$，$\phi(m_{1,p}, -m_{1,q})$，$\phi(-m_{1,p}, -m_{1,q})$のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすものを平文mとする（但し，$\phi$は中国人の剰余定理による$Z/(p)\times Z/(q)$から$Z/(pq)$への環同型写像を表す），

ことを特徴とする公開鍵暗号方法。

3．

請求項2において，

前記送信者は、前記平文m として、前記受信者へ送信するメッセージ文に対して，正しく復号されたかを確認するための検査情報を含めるステップを備える

ことを特徴とする公開鍵暗号方法。

4．

請求項3において，

前記送信者は、前記平文m として、前記受信者へ送信するメッセージ文に対して，予め定められた冗長性を持たせた内容を含め，請求項1の方法により暗号化するステップを備え，

前記受信者は，請求項1の方法により平文mを復号化し，予め定められた冗長性を確認するステップを備える

ことを特徴とする公開鍵暗号方法。

5．

請求項3において，

前記送信者は、前記平文m として、前記受信者へ送信するメッセージ文に対して，予め定められた冗長性を持たせた内容を含め、請求項２の方法により暗号化するステップを備え，

受信者は，請求項２の方法により平文m を復号化し，予め定められた冗長性を確認するステップを備える

ことを特徴とする公開鍵暗号方法。

6．

請求項２において，ランダム関数Hが公開されており，

前記送信者は，乱数情報を作成し、

該乱数情報に対して，排他的論理和およびデータの連接による演算を行い、

該演算により得られた結果をランダム関数Hに入力し，その結果を計算し、

該乱数情報と該ランダム関数への入力結果に対して排他的論理和およびデータの連接による演算を行い、

該演算を行った結果を，請求項２における乱数rと置き換え，請求項２における公開鍵暗号化方法の手順により暗号化する

ことを特徴とする公開鍵暗号における暗号化方法。

7．

請求項６の方法により暗号化した暗号文を復号化する方法において，

請求項２の公開鍵暗号方法による復号化手順を行い、

請求項６において行われた排他的論理和およびデータの連接による演算の手順の正当性を確かめ，

復号化結果を出力する

ことを特徴とする公開鍵暗号における復号化方法。

8.

送信者は，公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

受信者は、受信者側装置を用いた鍵生成のステップとして，

- $p$, $q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, $\beta$）を作成し，

- $\alpha, k \in \mathbb{Z}$
- $n = p^d q$　　($d$ は奇数)

なる公開鍵（n, k, $\alpha$）を作成し（但し，kはpqのビット長），

送信者は，送信者側装置を用い、平文m（$0<m<2^{n-k1}$）に対して，

$$m_1 = (m0^{k_1} \oplus G(r)) \,||\, (r \oplus H(m0^{k_1} \oplus G(r))) \qquad (0 < m_1 < 2^{k-2})$$

を計算し（但し，$G:\{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，$H:\{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする），Jacobi記号$a=(m_1/n)$，および，

$$C = {m_1}^{2\alpha} \bmod n,$$

を計算し，(C, a)を暗号文として前記受信者に送信し，

前記受信者は，前記受信者側装置を用い、前記秘密鍵（p, q, $\beta$）を用いて，暗号文(C, a)から，

$$m_{1,p} = C^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすxを$m'_1$として計算し（但し，$\phi$は中国人の剰余定理による$\mathbf{Z}/(p)\times\mathbf{Z}/(q)$から$\mathbf{Z}/(pq)$への環同型写像を表す），

$m'_1=s'||t'$（s'は$m'_1$の上位nビット，t'は下位$k_0$ビット）に対して，

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

を計算し，復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。また，復号結果が * であるとは，正しい復号ができなかったことを意味する）

ことを特徴とする公開鍵暗号方法。

9.

送信者は，公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

受信者は、受信者側装置を用いた鍵生成のステップとして，

- $p, q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$,，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成し，

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$
- $n = p^d q \qquad (d$ は奇数$)$

なる公開鍵（n, g, h, k, l, $\alpha$）を作成し（但し，kはpqのビット長），

送信者は，送信者側装置を用い、平文m（$0<m<2^{n-kl}$）および乱数r'（$0 \leqq r' \leqq 1$）に対して，

$$m_1 = (m0^{k_1} \oplus G(r)) \,||\, (r \oplus H(m0^{k_1} \oplus G(r))) \qquad (0 < m_1 < 2^{k-2})$$

を計算し（但し，$G:\{0,1\}^{k0} \rightarrow \{0,1\}^{n}$，$H:\{0,1\}^{n} \rightarrow \{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする），Jacobi記号$a=(m_1/n)$，および，

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n$$

を計算し，(C, D, a)を暗号文として前記受信者に送信し，

前記受信者は，前記受信者側装置を用い、前記秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n$$

を計算し，$\phi(m_1, p, m_1, q)$，$\phi(-m_1, p, m_1, q)$，$\phi(m_1, p, -m_1, q)$，$\phi(-m_1, p, -m_1, q)$のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすxを$m'_1$として計算し（但し，$\phi$は中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す），

$m'_1 = s' || t'$（s'は$m'_1$の上位nビット，t'は下位$k_0$ビット）に対して，

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする（但し，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。また，復号結果が * であるとは，正しい復号ができなかったことを意味する）

ことを特徴とする公開鍵暗号方法。

10．

送信者は，公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

受信者は、受信者側装置を用いた鍵生成のステップとして，

- $p, q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成し，

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　($d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）を作成し（但し，kはpqのビット長），

送信者は，送信者側装置を用い、平文m（$0 < m < 2^n$）に対して，

$$m_1 = (m \oplus G(r)) \,||\, (r \oplus H(m \oplus G(r)))　　(0 < m_1 < 2^{k-2})$$

を計算し（但し，$G:\{0,1\}^{k0}\rightarrow\{0,1\}^{n}$，$H:\{0,1\}^{n}\rightarrow\{0,1\}^{k0}$，は適当なランダム関数であり，$k=n+k_0+2$とする），Jacobi記号$a=(m_1/n)$，および，

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n$$

を計算し（但し，$F:\{0,1\}^{n+k0}\rightarrow\{0,1\}^{l}$は適当なランダム関数），(C, D, a)を暗号文として前記受信者に送信し，

前記受信者は，前記受信者側装置を用い、前記秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_1, p, m_1, q)$，$\phi(-m_1, p, m_1, q)$，$\phi(m_1, p, -m_1, q)$，$\phi(-m_1, p, -m_1, q)$のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすxを$m'_1$として計算し（但し，$\phi$は中国人の剰余定理による$Z/(p)\times Z/(q)$から$Z/(pq)$への環同型写像を表す），

$m'_1=s'||t'$（s'は$m'_1$の上位nビット，t'は下位$k_0$ビット）に対して，

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases}$$

を計算し，これを復号化結果とする（但し，

$$C' = m_1'^{2\alpha} g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n$$

であり，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。

また，復号結果が ＊ であるとは，正しい復号ができなかったことを意味する）

ことを特徴とする公開鍵暗号方法。

11．

請求項１０において，

前記受信者は，前記受信者側装置を用い、

$$C'_p = {m'_1}^{2\alpha} g^{F(m'_1)} \bmod p^d, \qquad C'_q = {m'_1}^{2\alpha} g^{F(m'_1)} \bmod q$$
$$D'_p = h^{F(m'_1)} \bmod p^d, \qquad D'_q = h^{F(m'_1)} \bmod q$$

を計算し，

$$C \equiv C'_p \pmod{p^d}, \qquad C \equiv C'_q \pmod{q},$$
$$D \equiv D'_p \pmod{p^d}, \qquad D \equiv D'_q \pmod{q}$$

により，(C, D)=(C', D')を検査する

ことを特徴とする公開鍵暗号方法。

12．

送信者は，公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

受信者は、受信者側装置を用いた鍵生成のステップとして，

- $p, q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成し，

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$
- $n = p^d q \qquad (d$ は奇数$)$

なる公開鍵（n, g, h, k, l, $\alpha$）を作成し（但し，kはpqのビット長），

送信者は，送信者側装置を用い、平文m（$0<m<2^n$）に対して，乱数r（$0<r<2^{k0}$）を選び，

$$m_1 = m \,||\, r$$

を計算し（但し，$F:\{0,1\}^{n+k0} \rightarrow \{0,1\}^l$は適当なランダム関数であり，$k=n+k_0+2$とする），

Jacobi記号$a=(m_1/n)$，および，

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n$$

を計算し，

(C, D, a)を暗号文として前記受信者に送信し，

前記受信者は，前記受信者側装置を用い、前記秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_1, p, m_1, q)$, $\phi(-m_1, p, m_1, q)$, $\phi(m_1, p, -m_1, q)$, $\phi(-m_1, p, -m_1, q)$のうち，$(x/n)=a$かつ$0<x<2^{k-2}$を満たすxを$m'_1$として計算し（但し，$\phi$は中国人の剰余定理による$\mathbb{Z}/(p)\times\mathbb{Z}/(q)$から$\mathbb{Z}/(pq)$への環同型写像を表す），

$$m' = \begin{cases} [m_1']^{k_0} & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases}$$

を計算し，復号化結果とする（但し，

$$C' = {m_1'}^{2\alpha} g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n$$

であり，$[a]^n$および$[a]_n$はそれぞれaの上位および下位nビットを表す。また，復号結果が＊であるとは，正しい復号ができなかったことを意味する）

ことを特徴とする公開鍵暗号方法。

13．

請求項12において，

前記受信者は、前記受信者側装置を用い、

$$C_p' = {m_1'}^{2\alpha} g^{F(m_1')} \bmod p^d, \qquad C_q' = {m_1'}^{2\alpha} g^{F(m_1')} \bmod q$$
$$D_p' = h^{F(m_1')} \bmod p^d, \qquad D_q' = h^{F(m_1')} \bmod q$$

を計算し，

$$C \equiv C_p' \pmod{p^d}, \qquad C \equiv C_q' \pmod{q},$$
$$D \equiv D_p' \pmod{p^d}, \qquad D \equiv D_q' \pmod{q}$$

により，(C, D)=(C', D')を検査する

ことを特徴とする公開鍵暗号方法。

14．

送信者側装置と、受信者側装置とからなり、前記送信者側装置は、公開鍵を用いて送信データを暗号化する手段を備え、前記受信者側装置は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する手段を備えた、暗号通信システムであって，

前記受信者側装置は、

- $p$, $q$：素数, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$, $gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成する秘密鍵生成手段と，

- $\alpha, g, h, k, l \in \mathbf{Z}$ $(0 < g, h < n)$
- $n = p^d q$ ($d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）（但し，kはpqのビット長）を作成する公開鍵生成手段とを備え、

前記送信者側装置は，平文m（$0<m<2^{k-2}$）および乱数r（$0 \leqq r \leqq 1$）に対して，

$$C = m^{2\alpha} g^r \bmod n, \quad D = h^r \bmod n$$

を計算する手段と、Jacobi記号a=(m/n)を計算し，(C, D, a)を暗号文として前記受信者に送信する手段とを備え、

前記受信者側装置は，前記秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算し，$\phi(m_1, p, m_1, q)$，$\phi(-m_1, p, m_1, q)$，$\phi(m_1, p, -m_1, q)$，$\phi(-m_1, p, -m_1, q)$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすもの（但し，$\phi$は中国人の剰余定理による$Z/(p)\times Z/(q)$から$Z/(pq)$への環同型写像を表す）を平文mとして出力する手段を備えることを特徴とする暗号通信システム。

15.

公開鍵を用いて送信データを暗号化する送信者側計算機と、前記公開鍵に対応する秘密鍵を用いて暗号化された前記送信データを復号化する受信者側計算機と読み込まれ、実行され、前記送信者側計算機と前記受信者側計算機とに、暗号通信を行わせるプログラムを格納した媒体であって、

前記プログラムは、

前記受信者側装置に、鍵生成のステップとして，

- $p, q$：素数，　$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，　$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，　$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成させ，

- $\alpha, g, h, k, l \in \mathbf{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　($d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）を作成させ（但し，kはpqのビット長），

前記送信者側装置に、平文m($0<m<2^{k-2}$)および乱数r（$0 \leqq r \leqq 1$）に対して，

$$C = m^{2\alpha} g^r \bmod n, \quad D = h^r \bmod n$$

を計算させ，Jacobi記号a=(m/n)を計算させ，(C, D, a)を暗号文として前記受信者に送信させ，

前記受信者側装置に、前記秘密鍵（p, q, s, $\beta$）を用いて，暗号文(C, D, a)から，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算させ，$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすもの（但し，$\phi$は中国人の剰余定理による$Z/(p)\times Z/(q)$から$Z/(pq)$への環同型写像を表す）を平文mとして出力させる

ことを特徴とするプログラムを格納した媒体。

16.

受信者側装置が持つ秘密鍵に対応する公開鍵を用いて、送信データを暗号化し、前記受信者側装置が暗号化された前記送信データを復号化する暗号通信システムに用いる送信者側装置であって，

前記受信者側装置が生成した、

- $p, q$：素数，$p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$，$gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$，$\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）に対応する，

- $\alpha, g, h, k, l \in \mathbb{Z}$　$(0 < g, h < n)$
- $n = p^d q$　　($d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）（但し，kはpqのビット長）を用いて、

平文m($0<m<2^{k-2}$)および乱数r（$0 \leqq r \leqq l$）に対して，

$$C = m^{2\alpha} g^r \bmod n, \quad D = h^r \bmod n$$

とJacobi記号a=(m/n)を計算し，暗号文(C, D, a)を生成する手段と、

前記暗号文(C, D, a)を前記受信者側装置に送信する手段と

を備えることを特徴とする暗号通信システムに用いる送信者側装置。

17.

送信者側装置が、秘密鍵に対応する公開鍵を用いて暗号化した送信データを復号化する、暗号通信システムに用いる受信者側装置であって，

- $p$, $q$：素数, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$
- $s \in \mathbb{Z}$, $gh^s \equiv 1 \pmod{pq}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$

なる秘密鍵（p, q, s, $\beta$）を作成する手段と、

- $\alpha, g, h, k, l \in \mathbf{Z} \quad (0 < g, h < n)$
- $n = p^d q \qquad (d$ は奇数)

なる公開鍵（n, g, h, k, l, $\alpha$）（但し，kはpqのビット長）を作成する手段と、

前記送信者側装置が、前記公開鍵（n, g, h, k, l, $\alpha$）を用いて、平文m($0<m<2^{k-2}$)および乱数r（$0 \leqq r \leqq l$）に対して計算した，

$$C = m^{2\alpha} g^r \bmod n, \quad D = h^r \bmod n$$

とJacobi記号a=(m/n)とから生成した，暗号文(C, D, a)を受信する手段

と、

前記暗号文(C, D, a)を、前記秘密鍵（p, q, s, $\beta$）を用いて，

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$

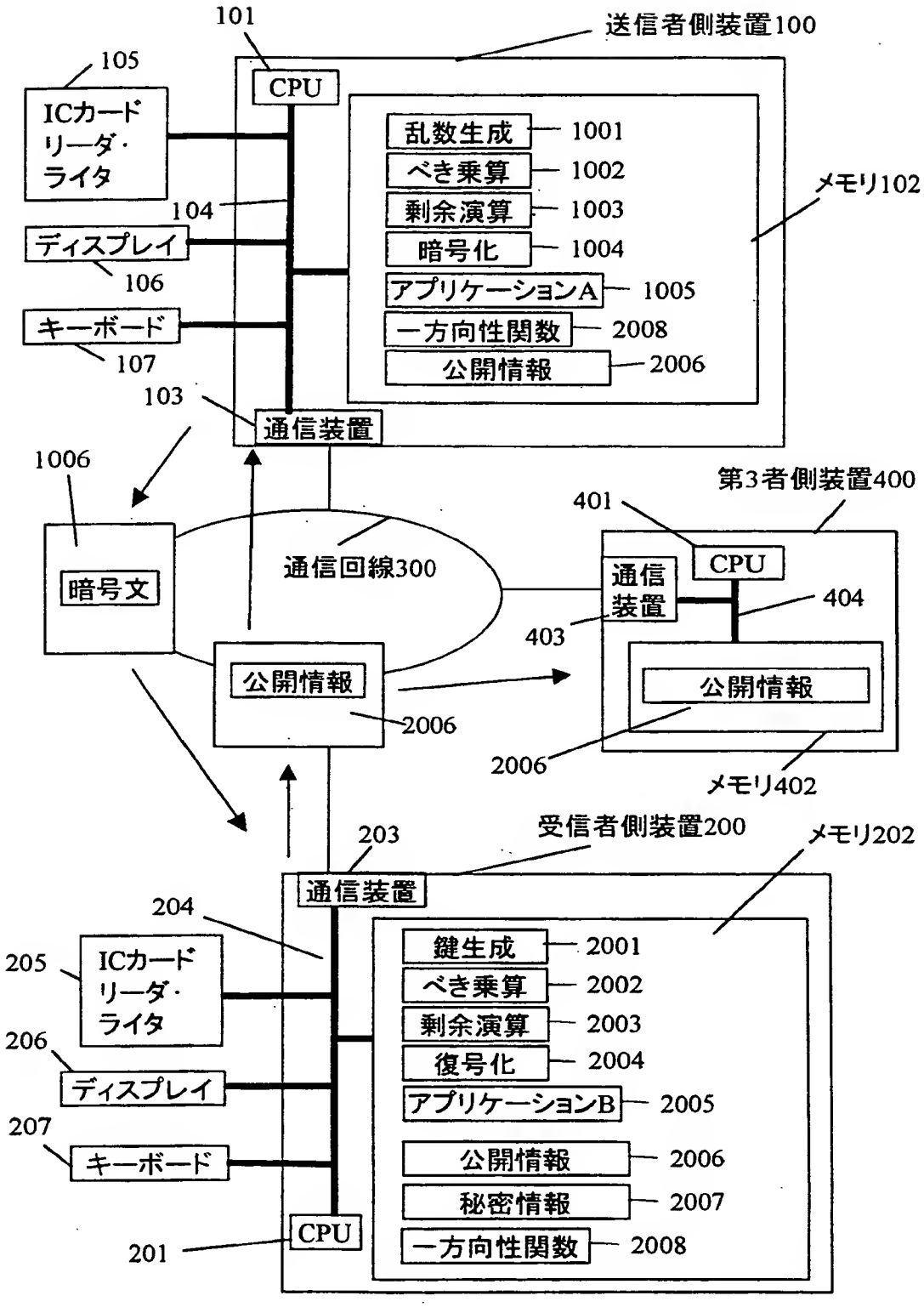
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

を計算する手段と、

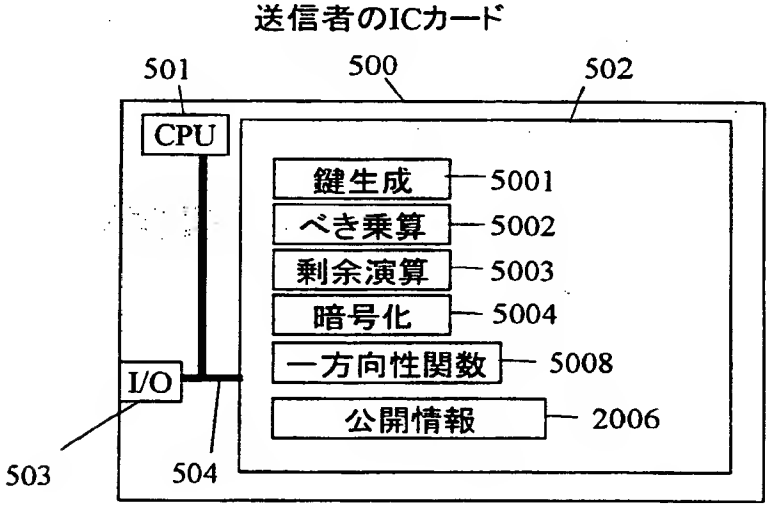
$\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$のうち，(x/n)=aかつ$0<x<2^{k-2}$を満たすもの（但し，$\phi$は中国人の剰余定理によるZ/(p)×Z/(q)からZ/(pq)への環同型写像を表す）を平文mとして出力する手段と

を備えることを特徴とする暗号通信システムに用いる受信者側装置。

第1図


101
送信者側装置100
105
ICカード
リーダ・
ライタ
CPU
乱数生成
1001
べき乗算
1002
剰余演算
1003
暗号化
1004
アプリケーションA
1005
一方向性関数
2008
公開情報
2006
メモリ102
104
ディスプレイ
106
キーボード
107
103
通信装置
1006
暗号文
通信回線300
第3者側装置400
401
CPU
通信
装置
404
403
公開情報
公開情報
2006
2006
メモリ402
203
受信者側装置200
メモリ202
通信装置
204
205
ICカード
リーダ・
ライタ
206
ディスプレイ
207
キーボード
鍵生成
2001
べき乗算
2002
剰余演算
2003
復号化
2004
アプリケーションB
2005
公開情報
2006
秘密情報
2007
一方向性関数
2008
CPU
201

第2図


送信者のICカード
501
500
502
CPU
鍵生成
5001
べき乗算
5002
剰余演算
5003
暗号化
5004
一方向性関数
5008
I/O
公開情報
2006
503
504

第3図

| | 暗号化 | 復号化 | IND-CCA2 |
|---|---|---|---|
| RSA | 約 2～1500 | 約 400 | No |
| ElGamal 暗号 | 約 3000 | 約 1500 | No |
| だ円暗号 | 約 120 | 約 60 | No |
| OAEP | 約 2～1500 | 約 400 | Yes |
| 本発明の方法 | 約 400（3） | 約 65 | Yes |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/00475

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7]
H04L 9/30 H04L 9/08 G09C 1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7]
G09C 1/00 - 5/00 H04K 1/00 - 3/00
H04L 0/00 - 9/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST(JOIS)
INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| T | Genji Nishioka, "Efficient and Security-provable Public-Key Cryptosystem", Research report, Information Processing Society of Japan, Vol.99, No.24, (05 March, 1999),pp. 25-30 | 1-17 |
| A | T. Okamoto and S. Uchiyama, "A New Public-Key Cryptosystem as Secure as Factoring, "Lecture Notes in Computer Science, Vol.1403, (1998), pp.308-318 | 1-17 |
| A | Y. Zheng and J. Seberry, "Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks," Lecture Notes in Computer Science, Vol.740, (1993), pp.292-304 | 1-17 |
| A | M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption," Lecture Notes in Computer Science, Vol.950, (1995), pp.92-111 | 1-17 |
| A | M. Bellare and P. Rogaway, "Minimizing the Use of Random Oracles in Authenticated Encryption Schemes, "Lecture Notes in Computer Science, Vol.1334, (1997), pp.1-16 | 1-17 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 10 April, 2000 (10.04.00) | 25 April, 2000 (25.04.00) |
| Name and mailing address of the ISA/ Japanese Patent Office | Authorized officer |
| Facsimile No. | Telephone No. |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/00475

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | S. Mueller, "On the Security of an RSA Based Encryption Scheme," Lecture Notes in Computer Science, Vol.1587, (1999), pp.135-148 | 1-17 |
| A | T. Takagi,"Fast RSA-Type Cryptosystem Modulo pkq," Lecuture Notes in Computer Science, Vol.1462, (1998), pp.318-326 | 1-17 |

国際調査報告

国際出願番号 PCT／JP00／00475

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl'
H04L 9／30　　H04L 9／08　　G09C 1／00

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl'
G09C 1／00 － 5／00　　H04K 1／00 － 3／00
H04L 0／00 － 9／38

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICSTファイル（JOIS）
INSPEC（DIALOG）

C. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| T | 西岡玄次 “効率的かつ安全性証明可能な公開鍵暗号方式” 情報処理学会研究報告, Vol. 99, No. 24, (1999年3月5日), pp. 25－30 | 1-17 |
| A | T. Okamoto and S. Uchiyama, “A New Public-Key Cryptosystem as Secure as Factoring,” Lecture Notes in Computer Science, Vol. 1403, (1998), pp. 308－318 | 1-17 |
| A | Y. Zheng and J. Seberry, “Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks,” Lecture Notes in Computer Science, Vol. 740, (1993), pp. 292－304 | 1-17 |

☑ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| 国際調査を完了した日 | 国際調査報告の発送日 |
|---|---|
| 10. 04. 00 | 25.04.00 |

| 国際調査機関の名称及びあて先 | 特許庁審査官（権限のある職員） | |
|---|---|---|
| 日本国特許庁（ISA／JP）<br>郵便番号100－8915<br>東京都千代田区霞が関三丁目4番3号 | 丸山 高政 | 5W 9570 |
| | 電話番号 03－3581－1101 内線 3576 | |

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 PCT／JP00／00475

C（続き）. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| A | M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption," Lecture Notes in Computer Science, Vol.950, (1995), pp.92－111 | 1-17 |
| A | M. Bellare and P. Rogaway, "Minimizing the Use of Random Oracles in Authenticated Encryption Schemes," Lecture Notes in Computer Science, Vol.1334, (1997), pp.1－16 | 1-17 |
| A | S. Mueller, "On the Security of an RSA Based Encryption Scheme," Lecture Notes in Computer Science, Vol.1587, (1999), pp.135－148 | 1-17 |
| A | T. Takagi, "Fast RSA-Type Cryptosystem Modulo $p^kq$," Lecuture Notes in Computer Science, Vol.1462, (1998), pp.318－326 | 1-17 |